Systemanskaffelse, udvikling og vedligeholdelse

Som softwarevirksomhed afhænger sikkerheden og pålideligheden af alle vores produkter af sikre kodningsprincipper og -processer for at sikre en smidig produktlivscyklus.

Vores livscyklus for sikker softwareudvikling omfatter:

- Eksternt bedømt design og kodning
- Stilmæssige retningslinjer
- QA-funktion/belastningstest
- Produkt- og forandringsstyring
- Evaluering af statisk kode (OWASP Top 10/SANS Top 25)

Derudover tilbyder vi følgende programmer for at sikre grænsen for vores tekniske arbejde:

- Sikkerhedsuddannelse af vores arbejdsstyrke
- Sikkerhedstest og -bedømmelse på implementeringsniveau
- Styrkede systemer
- Sårbarheds-/opdateringsadministration
- Test af web, program, sikkerhed

Teknisk arbejde

Analyse af softwaredesign

Komplet udvikling

Statisk inspektion af kode

Kvalitetssikring

Dynamisk analyse af programmet

Implementering

Implementering og stabilisering af programmet

Leverandørforhold

Håndtering af eksterne trusler i udkanten af vores funktionsområde medvirker til at sikre, at ingen yderligere risici tilføres organisationen gennem vores partner- eller leverandørforhold. Når det er muligt, vælger vi leverandører, der opretholder en international overholdelsesstandard for informationssikkerhed og/eller overholder samme værdier som Webfleet Solutions, når det kommer til beskyttelse af information og datafortrolighed.

Administration af informationssikkerhedshændelser

I tilfælde af en sikkerhedshændelse er det vigtigt at have en effektiv tilgang for at kunne håndtere hændelsen. Det indbefatter rettidig kommunikation til alle interesserede parter og rapportering af interne sikkerhedssvagheder for at understøtte en sikkerhedsgrænse, som beskrevet i forskellige gældende lovgivningsmæssige, regulerende og kontraktlige aftaler om notifikationer.

Informationssikkerhedsaspekter for administration af virksomhedskontinuitet

Vi administrerer et omfangsrigt program for kontinuitet for virksomhed og information for at sikre, at Webfleet Solutions-tjenesteplatformen er tilgængelig for vores kunder i tilfælde af en katastrofe. Via vores aktiv/aktiv-datacenterkonfiguration er risikoen for en større katastrofe i begge centre usandsynlig, da hvert center kan opretholde hele vores drift, hvis det skulle vise sig nødvendigt. Det betyder, at du kan stole på, at platformen er tilgængelig, når du har brug for det.

OVERHOLDELSE OG DATAFORTROLIGHED

Webfleet Solutions kontrolleres gennem vores Data Privacy Officer (DPO) for at sikre overholdelse af EU's generelle forordning om databeskyttelse samt anden gældende lokal lovgivning om databeskyttelse.

Vores ISMS-team (system til administration af informationssikkerhed) gennemfører jævnlige undersøgelser af lovgivningsmæssige eller sikkerhedsmæssige krav, der kan påvirke vores Telematics-platform eller informationsaktiver i henhold til ISMS' funktionsområde.

HIGHLIGHTS

- **MAKSIMAL SIKKERHED OG INTEGRITET**
  Dine data er i sikre hænder med vores ISO 27001-certificerede system.
- **BESKYTTELSE AF DRIVERFORTROLIGHED**
  Med vores fokus på databeskyttelse har vi samarbejdet med datafortrolighedsgrupper og arbejdsråd for at demonstrere vores engagement vedr. din datafortrolighed
- **DATASLETNING**
  Data markeres som fjernet og overskrevet i tilfælde af datasletning for at forhindre, at data gendannes af uautoriserede parter.
- **DATAFASTHOLDELSE**
  Som standard opbevarer vi alle data, herunder præcise dataspor i op til halvfems (90) dage, samt indeværende år plus to (2) tidligere år for vores logbog, dashboard og rapporter. Dette kan variere baseret på landespecifik lovgivning.
- **VÆLG INTEGRITET. BESKYT MILJØET**
  Vi gør vores del for at give dig en sikker platform, som giver dig mulighed for at spare omkostninger samtidig med, at du gør din del for miljøet.

Er du interesseret i mere detaljerede tekniske oplysninger relateret til vores sikkerhed og datafortrolighed? Du kan bede om at få hvidbogen "Certified Information Security and Data Privacy Telematics" på Webfleet Solutions' hjemmeside på **www.webfleet.com**

Kontakt os:
privacy@webfleet.com

CERTIFICERET INFORMATIONSSIKKERHED OG DATAFORTROLIGHED TELEMATICS

HOS WEBFLEET SOLUTIONS ER VI ENGAGEREDE I **INFORMATIONSSIKKERHED OG DATAFORTROLIGHED.**

Vi investerer løbende i vores tekniske arbejde, gennemprøvede teknologier, processer og mennesker, så vi kan sikre, at vi altid kan give dig den mest pålidelige Telematics-tjenesteplatform på markedet.

STYRKEN I WEBFLEET SOLUTIONS-TJENESTEPLATFORMEN

ISO/IEC 27001:2013-CERTIFICERET FOR INFORMATIONSSIKKERHED
Vores tjenesteplatform og modne processer er certificerede, så vores kunder kan nyde godt af det højeste niveau af beskyttelse for informationssikkerhed og datafortrolighed.

EV SSL-KRYPTERING MED HØJESTE STANDARD
Sikker, krypteret login og dataoverførsel til vores tjenesteplatform. Du kan stole på, at vores data er sikre og beskyttede

LOKAL INSTALLATION
Landsdækkende og internationale installatører

FØRSTEKLASSES SUPPORT
Fra lokale forhandlere og systemintegratorer

APP CENTER
Dokumenterede integrations- og tilføjelsesapps i App Center

Det er ikke overraskende, at vi er førende inden for flådestyring og Telematics.

Som en af verdens største udbydere af Telematics-tjenester er kontinuerlig forbedring af vores tjenester vigtigt for at sikre, at vi er den bedste partner for din virksomhed – nu og i fremtiden.

ISO 27001-certificeret funktionsområde

Vores ISMS-system (system til administration af informationssikkerhed) dækker alle vores kritiske forretningsprocesser, som vi skal bruge til at sikre informationsaktiver i forbindelse med Webfleet Solutions-tjenesteplatformen. Det omfatter arkitektur, teknisk arbejde, kvalitetssikring og it-tjenester, der leveres til Webfleet Solutions B.V. i vores teknologiske hovedkvarter i Tyskland samt vores sikre datacentre beliggende i EU. Dette er i overensstemmelse med ISO/IEC 27001:2013-standarden og er implementeret som beskrevet i vores Statement of Applicability-version fra november 2016.

"ISO 27001-certificeringen understøtter, at vi har fuld kontrol over vores processer, og endnu vigtigere, at vores kundedata er i trygge hænder, hvilket er afgørende for, at vi kan tilbyde en forretningskritisk "software som en tjeneste"-flådestyringsløsning."

Thomas Schmidt, Administrerende direktør, Webfleet Solutions

System til administration af informationssikkerhed

Hjørnestenen i Webfleet Solutions forpligtelse om informationssikkerhed er vores sikkerhedspolitikker og -programmer, der gælder for hele organisationen og for håndteringen af informationssikkerhed. Baseret på vores strenge risikostyringsprogram, der er tilpasset vores virksomhedsmål, arbejder vi med en veldefineret sikkerhedsgrænse inden for ISMS' funktionsområde, der indbefatter, men ikke er begrænset til, følgende emner:

INFORMATIONSSIKKERHEDSPOLITIKKER
Et detaljeret sæt sikkerhedspolitikker designet til at tilbyde administrationsledelse og support til informationsadministrationssystemet og alle driftsmæssige aktiviteter, som vedrører Webfleet Solutions-tjenesteplatformen.

ORGANISERING AF INFORMATIONSSIKKERHED
Informationssikkerhed har betydning for alle. Rollerne og ansvarsområderne for alle medarbejdere er baseret på informationssikkerhed. Sammen med et team, der arbejder fuld tid med informationssikkerhed, sikrer alle medarbejdere overholdelse og governance i henhold til ISO 27001, ensretning i overensstemmelse med EU's generelle forordning om databeskyttelse (GDPR) samt alle gældende lokale lovgivninger om databeskyttelse.

HR-SIKKERHED
Informationssikkerhed er afgørende før, under og efter opsigelsen af en medarbejder. Det indbefatter at vælge de rette medarbejdere og sikre dem vedvarende og tilpasset oplæring.

AKTIVSTYRING
Lager, ejerskab og vedligeholdelse gennem et aktivs livscyklus sikrer den rette kategorisering, mærkning og tilknytning af risikoejer. Det indbefatter sikker håndtering af virksomhedens intellektuelle ejendom og kundedata.

ADGANGSKONTROL
Igennem identitetsstyring begrænses al adgang til det, der er nødvendigt at have og nødvendigt at vide. Yderligere kontroller medvirker til at forhindre uautoriseret adgang. Systemlogføring og -overvågning kan f.eks. sikre registrering i realtid på tværs af vores sikkerhedsgrænse.

KRYPTOGRAFI
Vi investerer i avancerede hardware- og softwareløsninger. Testede kryptografiteknologier beskytter fortroligheden og integriteten af vores kundedata og driftssystemer.

FYSISK OG MILJØMÆSSIG SIKKERHED
Vi arbejder med to uafhængige Tier3+-datacentre i EU pga. de strenge krav til datafortrolighed. Vores testede aktiv/aktiv-konfiguration sikrer gendannelse efter katastrofer og højt tilgængelige funktioner, der testes med jævne mellemrum.

DRIFTSMÆSSIG SIKKERHED
Vi stræber efter at opretholde en styret, streng og repeterbar proces i vores drift. Ved at etablere basislinjer for sikkerheden håndteres risikoniveauerne og giver mulighed for en effektiv driftsmæssig gennemførelse.

Væsentlige faktorer for driftsmæssig sikkerhed:

- **Driftsprocedurer og dokumentation**
- **Sikkerhedskopiering/gendannelsestests af kritiske systemer**
- **Overvågning af driftsmiljøer**
- **Håndtering af hændelser, problemer og forandringer baseret på best practices**
- **Kapacitetsstyring med belastningstests**
- **Adskillelse af ansvarsområder**
- **Styrkede systemer**
- **Opdeling af miljøer til udvikling, test og produktion**
- **Sårbarhedsscanning**
- **Gennemtrængningsafprøvning**
- **Opdateringsadministration**

KOMMUNIKATIONSSIKKERHED
Datasikkerhed "under transport" kræver et sikkert netværk, som dataene kan bevæge sig igennem. Vi gør brug af sikre kommunikationsmetoder såsom:

- **Netværksadskillelse**
- **VLAN-opdeling, DMZ med firewalls på flere niveauer**
- **Network Access Controls (NAC)**
- **Kryptering som standard med brug af de nyeste branchestandarder**